Pages 1 - 48

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE RICHARD SEEBORG

MICHAEL KATZ-LACABE, et al.,	)	
	)	
Plaintiffs	)	
	)	
vs.	)	No. C 22-04792 RS
	)	
ORACLE AMERICA, INC.,	)	
	)	San Francisco, California
Defendant.	)	Thursday
	)	February 9, 2023
	)	1:19 p.m.

TRANSCRIPT OF PROCEEDINGS BY ZOOM WEBINAR

APPEARANCES:

For Plaintiffs:

LIEFF, CABRASER, HEIMANN & BERNSTEIN LLP
275 Battery Street - 29th Floor
San Francisco, California 94111

BY: DAVID T. RUDOLPH, ATTORNEY AT LAW
MICHAEL W. SOBOL, ATTORNEY AT LAW
JALLE H. DAFA, ATTORNEY AT LAW
NABILA ABDALLAH, ATTORNEY AT LAW

For Defendant:

MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105

BY: TIFFANY CHEUNG, ATTORNEY AT LAW
DANIELLE E. VALLONE, ATTORNEY AT LAW

Reported By: ***Debra L. Pas, CSR 11916, CRR, RMR, RPR***
Official Reporter - US District Court
Computerized Transcription By Eclipse

Thursday - February 9, 2023 **1:19 p.m.**

P R O C E E D I N G S

---000---

THE CLERK: Calling case 22-CV-4792, Katz-Lacabe vs. Oracle America.

Counsel, please state your appearances starting with the plaintiffs.

MR. RUDOLPH: Good afternoon, Your Honor. This is David Rudolph from Lieff, Cabraser, Heimann & Bernstein on behalf of the plaintiffs, and with me are my colleagues Mr. Michael Sobol, Jalle Dafa, and Nabila Abdallah.

THE COURT: Good afternoon.

MS. CHEUNG: Good afternoon, Your Honor.

THE CLERK: Please go ahead.

THE COURT: Ms. Cheung, go ahead.

MS. CHEUNG: Good afternoon, Your Honor. This is Tiffany Cheung of Morrison & Foerster on behalf of defendant, and with me is my colleague Danielle Vallone.

THE COURT: Good afternoon.

So this matter is on for the Defendant's Motion to Dismiss the Class Action Complaint. I have reviewed what you've submitted for me.

So why don't I just start with the moving party, and I don't know if that's Ms. Cheung or Ms. Vallone that wants to start the discussion.

MS. CHEUNG: I'll go ahead and start, Your Honor. Thank you.

THE COURT: Very good.

MS. CHEUNG: Oracle has moved to dismiss the entire complaint in this action for several reasons.

The first that applies to all the causes of action, and there are a few arguments where the grounds applied will apply to the entire complaint so we'll start with those and then turn to the claim-specific arguments.

But the first is lack of standing. The plaintiffs have not alleged Article III standing in order to bring the claims that they are alleging before this Court, and what the -- at a very fine level, Your Honor, what the plaintiffs are alleging here is a very generalized attack on what they believe is an improper action by the ad tech industry as a whole.

They cite to a number of different unpassed laws. They cite to policies that they believe should reflect the law but do not actually reflect what the law is today, and so they seek to dramatically expand what the laws actually protect through this lawsuit and this court.

THE COURT: Let me start you with -- just focus you on -- let's take the named plaintiff, Mr. Katz-Lacabe. So he avers that he was notified that Oracle has created this electronic profile of him without his consent.

Why doesn't -- why isn't that satisfactory to show that

the conduct of the defendant is traceable to the injury that Mr. Katz-Lacabe -- and he goes through various aspects of why he feels that -- contends he's been injured -- why isn't that enough of a line of causation for standing purposes?

MS. CHEUNG: Yeah. Thank you, Your Honor.

For the first -- first of all, Mr. Katz-Lacabe does not identify with any specificity any harm that he actually suffered.

So the Complaint is rife with allegations of generalized harm that someone else, some unidentified individual, may have suffered, but plaintiff Katz-Lacabe -- we'll focus on Katz-Lacabe for now -- doesn't -- because none of the other plaintiffs do this either, but doesn't actually identify any harm that he himself suffered, and that's required for Article III standing at the pleading stage. So that's the first issue.

The second is the traceability issue that Your Honor previewed. They -- the plaintiffs admit that there are -- the way that this works, and this is what they concede, they allegedly put information into websites that are owned by third parties, not Oracle, and that the information that they put onto websites owned by third parties, what happened is those parties allegedly put some kind of cookie or pixel or, you know, we'll just generalize that for now, that allowed Oracle to allegedly get information.

But in order for -- but as plaintiffs concede, the way this works is that a third party had to intervene in the causal chain. Some third party, some identified third party -- unidentified third party -- and that's important too -- they concede that there was a third party that put some kind of code onto a website owned by that third party and thereby Oracle was able to obtain information, but there's no -- there's absolutely no specificity as to what website plaintiffs allegedly put this information in and whether they consented to allowing that third party to share that information.

So they -- there is this huge logical leap between they put information on a third party's website and then there is absolutely no traceability to eventually Oracle getting that information and vented through the website.

THE COURT: Okay. Going back to your first point about the -- what you perceive to be the absence of identifiable injury here, we will come to it, but, as I understand it, the 17200 standing -- narrower standing question does require some averments of economic injury, but that's not necessary for Article III standing.

So why isn't it enough that they -- that -- and perhaps it could be something that could be fleshed out by amendment -- but that suffered harm in the sense of emotional distress and the like? I mean, why isn't that enough?

MS. CHEUNG: Your Honor, we understood that the

standing requirements for UCL are quite strict, and we'll certainly get to that and they clearly don't meet that.

But even as to the Article III standing injury, they need to specify that they suffered that harm, and they haven't done that in this complaint. And we could speculate as to what type of harm they might claim that they suffered and whether that's sufficient or not, but that would be speculation at this point.

THE COURT: Well, would emotional -- emotional injury be sufficient if they averred it? I know your contention is think haven't averred it, but if they did aver it, would that be enough?

MS. CHEUNG: I think, Your Honor, there is some type of injury that might be -- that might suffice for Article III standing if they averred that injury as to themselves and it was connected to Oracle and it was connected to being caused by Oracle and not by this intervening third party or, frankly, by some other data broker.

Because they also allege that there are all these other data brokers in the world that are doing the same things Oracle is doing, and there's absolutely no connection between whether the information they put on this website and may have consented to either got to Oracle or got to some other data broker that then allegedly caused some harm they don't identify.

So there are so many missing gaps in this link, Your Honor, they can't possibly satisfy Article III standing

based on the complaint as they've alleged it.

THE COURT: Before we barrel ahead on these other claims for relief and, you know, I need to stay within the bounds of the Complaint, but could you give me from your perspective what Oracle is doing here?

I mean, in terms of, you know, the plaintiffs identify the Oracle ID graph and the Oracle data marketplace, and I'm unclear are they -- and I'll ask them this too -- are these separate operations? Are they overlapping? What are they?

MS. CHEUNG: Yes, Your Honor. So starting again at a high level because before we get into the weeds, Oracle serves as a service provider to these website operators. So, again, third parties not at issue in this case. What plaintiffs are alleging is that they put information into certain unidentified websites.

Assuming for the -- for purposes of this argument that they actually identify those websites, what Oracle does generally do for some websites, may or may not have been the websites plaintiff actually used; but for some websites is they are a service provider where they can for these third parties collect certain information about individuals with their consent.

Because Oracle does require that if these websites are collecting information, that they to so with appropriate consent; but if they do --

THE COURT: To that party, not to Oracle. There's no consent to Oracle here.

MS. CHEUNG: It -- there -- well, the requirement is that the third party obtain whatever consent is necessary in order for that third party to share, do what it's doing. That's the requirement.

So if that information is shared with Oracle, they're required to get the consent to be able to share that information with Oracle. So that's required.

And so that is --

THE COURT: Not to, again, get too much in the weeds, but how is that reflected? Does Oracle require them to produce some sort of proof of that or do they just say "You're required to do it" and then they assume they do it?

MS. CHEUNG: It is -- it is reflected -- and, again, to stick to the papers at hand --

THE COURT: Right.

MS. CHEUNG: -- it's in Exhibit B of the Request for Judicial Notice, which of course is cited in the -- in the Complaint and incorporated by reference.

THE COURT: Right. Now, by the way, just to digress for a moment -- and this is --

MS. CHEUNG: Sure.

THE COURT: -- going to be something that overlays a lot of this -- this is an issue in which I am -- I have strong

views, and that is the -- what I consider to be the overuse to a very large degree of judicial notice, particularly in pleading motions, but we also know that there's a distinction between that and incorporation by reference.

Incorporation by reference, which is a different concept, and I understand that if something is truly incorporated, it can be -- it can be referred to for pleading purposes, that isn't just if there's a reference to something, it's open season on everything in that -- on those materials is now subject to being considered.

And I will tell you that I think you throw the net too far with what you want me to take either through incorporation of judicial notice. It's -- you know, the classic incorporation by reference is you attach the contract to the Complaint and the Complaint talks about the contract and, therefore, that is incorporated by reference.

But a whole host of policy -- privacy policies which may be referenced, everything in those policies doesn't become something I can use for purposes of a Motion to Dismiss.

So, in any event, I just want you to know that that is my view. So Exhibit B, I think you've got a good argument on, I think J and H. I'm not so sure about the other exhibits.

So that is background. Go ahead, Ms. Cheung.

MS. CHEUNG: Okay. Understood, Your Honor. And we can certainly go through the exhibits.

To your point, perhaps there are different arguments that apply to different exhibits.

But as to Exhibit B, that is where it is very clear that Oracle requires any website operator that is using the products that Oracle offers to these websites to get the appropriate consent to cover the conduct that that website is operating. That independent website decides to do what it's going to do with the information that consumers provide, and they're required to get consent.

So that is at a very high level what Oracle is doing. It's merely a service provider.

THE COURT: When it's doing that, it's under the auspices of which of its programs? This ID graph? This data marketplace?

What is it that you've just described for me, what would be the pigeonhole that Oracle would identify for this operation you've generally described?

MS. CHEUNG: Right. So the specific products that are at issue or at least identified in the Complaint are very different.

So BlueKai is probably the one that the plaintiffs point to the most. So that is, in our view, what they seem to be challenging, you know, most -- most in high priority.

The others are also mentioned, but they're different in that other -- the other programs, such as they mentioned this

Moat Analytics, for example, I mean, it's a -- that is very different in that it's a high-level analytics tool that is not tied to any individual period but provides statistics or metrics on how -- how frequently, perhaps, and I'm using an example, but how frequently a consumer or a group of consumers viewed a certain ad. You know, how -- how many clicks did that ad get, for example.

So the other products are quite different in certain ways, but the one that seems to be the key, at least from our read of the Complaint, is this -- this BlueKai product.

THE COURT: Okay. It's fair, though, to understand this, if I'm reading it correctly, that this is not just a situation which Oracle is providing some software to some third-party user's customers of Oracle so that they can do a collection of data; that Oracle is using the information that finally comes back to Oracle from these third parties and then sells it, don't they?

MS. CHEUNG: Well, I mean, what is alleged is that what Oracle is doing is providing a service for these third parties so that they can -- so that they can figure out what type of advertising is going to be of greatest interest to those who are on their website.

THE COURT: Understood.

MS. CHEUNG: So if I'm on a website and I am showing interest in a certain product, that website is able to use

Oracle's products to identify that I'm actually very interested in this product, and so I would rather get this ad than some other random ad they --

THE COURT: And I'm not suggesting -- I'm just talking about what they are claiming. You may say this isn't what's happening, but it would be a very different proposition if all they were claiming is that Oracle was providing the wherewithal to these third parties so that the third parties could analyze the data and come up with some conclusions about the usefulness of their advertisements and the like.

They're averring anyway that you're doing a lot more than that; correct? You're taking the information and you're monetizing that information and using it in the marketplace.

Now I know you may say "That's not what we're doing," but isn't that what they're saying you're doing?

MS. CHEUNG: So they are -- they are -- they -- I agree that they are alleging that in a very generic -- at a very generic level. At a very generic level.

So they are alleging that that is what is going on without any real specificity or basis in actual fact allegations and also as to in lumping in Oracle improperly with what data brokers in general do or what the industry does.

So to the extent that they're averring it, it is not specific enough as to what Oracle is doing as opposed to some other data brokers or some other actors in the industry with

which they have an issue with. So that's -- that's where we think this -- well, one of the reasons why this complaint is deficient.

THE COURT: Okay. Going beyond standing and going into your arguments that they've failed to state a claim, you know, 17200, as we've kind of alluded to, I know it has a bit of a different standing, a narrower standing, parameters. We don't have to talk about that.

The other issue, and there's a back and forth about whether or not unjust enrichment is a stand-alone. I see that so many times, but the law is quite unsettled I'll acknowledge. And then there's a dec relief claim, and let's put those aside for a moment.

What I'd like to -- you to tell me a little about is the Wiretap Act, the California Invasion of Privacy Act claims -- I think they're four and five of the claims for relief -- and then inadequacies with respect to the -- you know, the California claims. So if you can talk about that for me.

MS. CHEUNG: Okay, yes. Yes, Your Honor.

And if you have questions, Your Honor, or you'd be interested in hearing argument with respect to extra-territoriality, so that's related to the California claims --

THE COURT: You're talking about the California -- whether or not that you can have non-California plaintiff --

MS. CHEUNG: Yes.

THE COURT: -- participants?

Yeah. I mean, we can talk about that a bit. I don't think that it's at the pleadings when we adjudicate that question, but I think it's a legitimate question.

My -- where I may part company with you is I don't think this is the time to ferret all that out, but, okay, go ahead.

MS. CHEUNG: If I could address that briefly --

THE COURT: Go ahead.

MS. CHEUNG: -- and then I'm happy to address the specific claims as well.

Because I do think that particularly where, even based on the allegations -- oh, even based on the allegations, the plaintiffs are relying very heavily on the locus of Oracle's headquarters in California as, you know, emanating all of this activity.

So obviously, first of all, we don't believe that that's where the locus of the activity emanated from because of the -- because of the fact that each individual consumer was in their home on their browser allegedly giving information in whatever state they were in or country.

I mean, the reason why this doesn't matter, Your Honor, is they're alleging a global class.

THE COURT: But that's an argument for you can never have a class action in this kind of a case because of the wide

geographical location of all the potential putative plaintiffs. Is that -- I mean, that's the logical extension of your argument. If they're all over the place, well, you can never go anywhere.

MS. CHEUNG: Well, not for this type of claim. I mean, this -- we are not arguing that you could never have it but for the claims at issue here, which relate to where an individual's privacy allegedly was violated and when the last act occurred which then triggered an alleged violation.

So we're certainly not saying it could never happen, but we're focused on the allegations in this case that what happened is an individual consumer sitting in their home in allegedly Ireland put information into a website and when that info- -- when they did that in some other country and it was shared, that somehow California law could apply to that resident.

That's where we -- that's where we don't agree. We don't agree that in this case for these claims California law can apply to a worldwide class, which is what they're alleging.

THE COURT: And you think -- you'll point me to -- and I'll go back and look at your papers -- where that issue has been addressed on a Motion to Dismiss as opposed to class certification or summary judgment or something like that?

MS. CHEUNG: Yes, Your Honor. The cases that we cite to in our papers were a Motion to Dismiss.

THE COURT: Okay. I'll go back and look. Go ahead.

MS. CHEUNG: The other point I would make about that on California is that Oracle is now headquartered in Texas and has been since 2020, which the plaintiffs concede in Paragraph 10 of their Complaint.

So even if somehow we could assign, you know, where the headquarters is as the place where that law is going to apply worldwide, Oracle's headquarters moved in 2020; and based on, let's take Plaintiff Golbeck's own allegations, she didn't receive -- Golbeck didn't receive information about -- information Oracle that -- allegedly possessed until March of 2022. So well after Oracle's headquarters were no longer in California.

So for that reason as well, it does not make sense to apply California law to a global class when even based on what they're relying on, which is the company's headquarters, that was not the case during the time of the alleged violations to plaintiff. So we make that point as well.

But turning to the specific causes of action, starting with the California claims, the -- the intrusion upon seclusion and the invasion of privacy claim largely have overlapping tests, and I'll just address those together.

But the issue there is that they've got -- plaintiffs need to be able to plead a reasonable expectation of privacy. So that's the first.

And the second is that -- that the alleged conduct was highly offensive and egregious.

So plaintiffs fail on both, on both required elements, with respect to this pleading.

First, with respect to a reasonable expectation of privacy, they agree that the relevant factors are the sensitivity of the data and the manner of the collection of the data.

So with respect to the sensitivity of the data, they identify things like app usage data, contact information, home location device data. None of that rises to the level of sensitivity that is sufficient to show an invasion of privacy claim.

Though they do, we acknowledge, allege in conclusory fashion that there is sensitive data like biometric information, genetic information, pregnancy information, religious, political information that could be at issue, it is fully conclusory. Not at all -- not at all tied to anything the plaintiff experienced. Not at all tied to anything that Oracle collects for anybody, but wholly conclusory. So on the sensitivity factor, they fail there.

As to the second factor, which is the nature of the manner of the collection, they also haven't alleged that the nature of the manner of the collection rose to the level of a reasonable expectation of privacy.

They cite very -- they rely very heavily on the Ninth Circuit's ***Facebook*** decision, so I feel that I need to address that. But that decision was very different from this case, where that case and the Ninth Circuit and other -- other courts following that decision have very expressly relied upon the fact that Facebook allegedly tracked information as to users after the users were logged off of Facebook.

And the critical distinction there, which several courts have said this was critical in that case, was that Facebook represented it would not be tracking users after they logged off.

So contrary to those representations, they allegedly did something that was not consistent with their own representations, which then led to a reasonable expectation of privacy. That is not the case here.

But the plaintiffs here do not allege that Oracle promised that it was not going to collect any information, promised that it wouldn't do all the things that they claim that Oracle does. And, in fact, Oracle does disclose it.

And understanding that Your Honor may not look at the privacy policy that we've -- that we've attached, even beyond that, Oracle disclosed it and they don't -- they don't allege otherwise. They do not allege that Oracle somehow misrepresented what it was doing. So they failed on the reasonable expectation of privacy.

On the second factor, which is whether it's highly egregious, we cited to multiple cases that show that the collection of browsing and internet history data, it does not rise to the level. App usage data does not rise to the level. Identifying contact information, device data, none of that is highly egregious.

According to our social norms where we live in a world where we know that certain of our information is shared, and that type of information does not rise to the level of an invasion of privacy.

Now -- so plaintiffs don't meaningfully dispute that. What they say is: Well, the aggregate of all that information together does somehow rise to the level of an egregious invasion of privacy, but they don't cite to any cases that actually say that.

And, Your Honor, you know, where there's pieces of information that don't rise to the level, zero plus zero is still zero if you add it all together. They don't cite to anything that actually supports their theory that somehow this data that doesn't rise to the level in the aggregate otherwise would rise to the level of an egregious breach.

Those are the California privacy arguments, Your Honor, or privacy claims. I'm going to November on then, unless you have questions, Your Honor, to the --

THE COURT: Go ahead to the --

MS. CHEUNG: Okay.

THE COURT: -- wiretap and CIPA.

MS. CHEUNG: Yes.

So on the wiretapping claims, let me start with the Federal Wiretap Act because I think that's -- well, there are -- there are -- there are defenses to both, but that one I think I can address very quickly in that it's a one-party consent statute.

So they don't dispute that the third-party websites for whom they gave information --

THE COURT: Right.

MS. CHEUNG: -- consented to the collection of the information because, of course, they say they are Oracle's customers. Oracle's customers did, in fact, consent to the transmission of that information, and that's a defense to the Federal Wiretap Act.

Their -- their next argument is that somehow the crime tort exception applies because, again, with no basis they argue that Oracle had the purpose of committing a crime. That is absolutely nowhere in the Complaint at all, that there was some criminal activity.

THE COURT: Step back for one moment to the one-party consent notion. Isn't their answer to that -- you're sort of suggesting that the plaintiffs are somehow what? Have a connected agency? They get the -- they get hoisted by the fact

that the third party is, as you say, consenting. But isn't their point they're not the third -- they're separate and apart from the third party?

MS. CHEUNG: Well, so their -- my -- the way that this should be framed is to look at who are the parties to the communication. What they allege is the parties to the communication are, in their view, the individual consumer and the website operator. Those were the two parties to the communication they believed was going on; and with respect to those two parties, the third-party website operator consented to Oracle's --

THE COURT: So if anybody in the chain of events consents, then we don't have to go further. We don't have to determine whether or not the -- the -- it's -- the consent is imputed to Oracle or not. It's just once we find somebody who's consenting, the Federal Wiretap Act is not at issue anymore; right?

MS. CHEUNG: That's right, which is why it's a one-party consent statute. There are other statutes for which one party wouldn't be enough; but under the Federal Wiretap Act, that is enough in that to keep that claim.

With the CIPA claim, it's a -- it's a similar argument, although it's slightly different. The issue there is that Oracle, as I explained earlier, is a service provider. So Oracle is a party to the communications in that it is a service

provider to the third-party website operator. And in that role -- in that role, if it's a party to the communications because it's just merely acting as a service provider to the website, there's no CIPA claim because there's no introspection by a third party. Oracle is stepping in the shoes and acting as an agent for the website operator. So that's why those claims also fail.

In addition, with respect to the CIPA claim, they also don't allege that there were contents of the communication which were shared because you -- plaintiffs cannot -- it's not just any information that was shared that would constitute coverage under the CIPA claim but only certain contents.

So record information related to the transmission is not do going to be enough. They cite to a couple of things in saying that there were contents. They, frankly, acknowledge that most of what they claim was shared does not rise to the level of contents, but they say: Well, the refer URLs could be contents. The problem there is that although there are some cases that suggest that some information in URLs could constitute contents, some say: Well, no. If the URLs don't include anything more than record information, then that wouldn't -- that wouldn't constitute contents under the statute.

And plaintiffs do not allege at all what they think was transmitted in the, quote/unquote, "referral" -- "refer URL."

And it is not the case that every URL would constitute contents under the statute.

Same issue with the entry of data into web forms which they say must be a communication; but without specificity as to what type of information was transmitted, if it was only information that would not otherwise constitute contents, then it's not covered by the statute.

And then I can address the UCL unless Your Honor --

THE COURT: Why don't I -- let me hear from plaintiffs, and then we'll come back to you if we need to get some more on that.

Who on the plaintiffs' side wants to --

MR. RUDOLPH: That would be me, Your Honor.

THE COURT: Go ahead, Mr. Rudolph.

MR. RUDOLPH: Thanks.

So there are four points that I'd like to discuss, and the first has to do with the reasonable expectation of privacy and more generally what this case is about. And then I'd like to explain why Article III standing here is abundant, it's not really a close call. And then I will explain why consent is wholly absent here. And, finally, I'd like to explain why this is really highly egregious conduct and the claims here are not contrary to Oracle's framing of this seeking to sort of blaze new legal trails but really just seeking to enforce rights and statutes that have been on the books for decades if not over a

century.

So first with respect to the reasonable expectation of privacy, plaintiffs have no choice but to conduct a large portion of their lives online. And one point that I want to be very clear that's very important and that Oracle seems to rely repeatedly is that we're not just alleging that Oracle collects online activity with websites. It collects browsing history, but it also collects offline activity. It collects address information. It collects purchases in stores. It collects physical movements in stores. It collects -- essentially everything that could be an electronic record of your activities is part of what Oracle is collecting, and --

THE COURT: But isn't there point a lot of -- much of that you don't have an expectation of privacy? Your information, your address information and the like, that you're utilizing in the internet world is not expectation of privacy.

MR. RUDOLPH: While there might not be an expectation of privacy in some of the individual pieces of data, I think *Facebook Tracking*, which is -- I do think is really sort of on all fours with this case in many ways held that individual's main expectation is that entities will not be able to collect broad swaths of personal information absent consent. That -- that -- that is the essence of the reasonable --

THE COURT: Is it enough to just -- you know, I did read through the Complaint, you know, with some care and it has

a lot of averments about: Oh, we -- in the modern age, we conduct our lives on the internet and it's ubiquitous and it is critical and nobody can do anything without it. But don't you have to do a lot more than the very general proposition that that's how modern-day life is conducted?

I mean, that -- it's almost saying: And, therefore, there must be a lot of private stuff in there. And you've got to be more specific than that, don't you?

As Ms. Cheung alluded to, if you were talking about the specific retrieval of medical information, you know, you allude to the notion that there's -- there is information potentially pertaining to sensitive issues like reproductive questions and all the like, but don't you have to be specific about that?

MR. RUDOLPH: So we do allege that Oracle collects information related to sensitive categories like religion, health, politics, et cetera.

We also allege that the plaintiffs -- the plaintiffs received these documents from Oracle showing that they were tracked and their data was analyzed.

Really what this case is about is the fact that the information is being collected and then what Oracle is doing with it based on what it tells the world it does with it.

So Oracle explains that it collects this sort of information. It collects -- it makes it available to third parties. It analyzes it and turns it into these detailed

dossiers.

And to get back to your question, in addition to that sensitive information, there is -- there is precedent, including ***Facebook Tracking*** and including ***Carpenter*** that suggests that when the data that's being collected reaches a certain critical mass, a certain level of specificity, that a privacy interest is at play there.

THE COURT: Why don't you take up Ms. Cheung's specific point with respect to the ***Facebook*** case where she says the critical distinction which you're missing here is continual tracking when the -- effectively the representation is that collecting and tracking has stopped, and that's what the court was focused upon.

MR. RUDOLPH: Your Honor, I think that interpretation of the case sort of completely turns the law on its head. The point there was that these are -- these are companies that the plaintiffs were in privity. They weren't browsing the Facebook platform. They were off platform. They thought people other -- companies like Facebook or Google were not -- were not tracking them.

That doesn't mean that in order to have a reasonable expectation of privacy you have to have some sort of contractual representation from a party that they are not -- that they are not surveilling you.

It -- it -- what's salient about the fact that they made

these representations is that the plaintiffs then just didn't believe they were -- it was another party that was -- that was surveilling them.

So -- okay. So to get to sort of how this works, this case is rests on -- it's based on two factual pillars. These pillars, they interact with each other but they are independent bases for legal claims. And the first has to do with the collection of plaintiffs' data including through methods that we allege violate the wiretap laws.

And then the second has to do with the creation, taking that data and then combining it with other sources of data like the offline data, like geolocation data, and creating these dossiers that is facilitated through the ID graph that is designed specifically to take disparate pieces of information from all over the web, including from different devices, and following people across different devices and then selling that information to third parties through the data marketplace.

So what Oracle is doing is really a form of surveillance that the voters of California made a decision 50 years ago to make illegal by amending the Constitution, and we discuss in the Complaint and also cite to the ballot measure.

Your Honor, I would like to with your permission share my screen because I -- we did pull up the ballot measure itself, and there's some language in there that I think is relevant.

(Document displayed.)

THE COURT: Why don't you just tell me what it is.

MR. RUDOLPH: Okay. My apologies? Is it up now?

THE COURT: Yes.

MR. RUDOLPH: Okay. So you can see down at the bottom the highlighted language notes that computerization of records makes it possible to create cradle-to-grave profiles on every American; at that at present there are no effective restraints on the information activities of government and business, and this amendment creates a -- I know a word is missing there but it's "legal" -- a legal and enforceable right of privacy for every Californian.

THE COURT: You're pointing me to some arguments in favor of the -- I mean, I don't think -- I know you say that's some legislative history or something? I mean --

MR. RUDOLPH: It is --

THE COURT: -- what's the language of the proposition that arguments -- I don't think an assemblyman who's written and the state senator who then went on to be mayor who is writing why they believe this is important is the force of law. Why do I even look at it, to be honest with you?

MR. RUDOLPH: Because it's a ballot measure, there is no legislative history for it. The California --

THE COURT: That's my question. Is this -- I'm not comfortable with the idea that arguments in a ballot pamphlet are tantamount to legislative history.

MR. RUDOLPH: The California Supreme Court has specifically noted that this ballot measure is essentially the recognized legislative history of the ballot measure, and there is a number of cases that quote this language in some detail.

THE COURT: Well, I thought you were going to show me the language of the proposition that was approved by the voters. What is that language?

MR. RUDOLPH: That is amending the California Constitution to add the word "and privacy" to the --

THE COURT: That's it. That's all it is; right?

MR. RUDOLPH: Right. Right. Right. Right.

But the -- the point is that the reason that that was being added was to protect the voters and future generations from the creation of these sort of cradle-to-grave profiles that -- that -- which is exactly what Oracle is doing now.

And this is -- this ties into the notion of the reasonable expectation of privacy. You noted they just said the word "and privacy." What does that mean? In this context, it means you have a reasonable expectation of privacy to be free from the sort of pervasive electronic surveillance that now 50 years later we've gotten to the point where a company such as Oracle is actually engaging in it.

THE COURT: Yes. But isn't -- but, again, going back to an earlier question of mine, you're pointing with a very broad brush. There is the mining, if you will, of information

that you would -- that no one would argue you would have a reasonable expectation of privacy regarding, and then there is material information where you do. You're not -- and it's more -- it's a question, not a statement.

You don't think you need to be more specific than painting this very broad brush that Oracle retrieves and uses all sorts of information about people; and just almost asking me to assume that within that information, there is some information for which a person would have an expectation of privacy.

MR. RUDOLPH: Well, in the Complaint we do describe quite a bit of specificity about the type of sensitive information that Oracle is collecting. I mean, that's described in detail. The general statement of facts is, you know, Paragraphs 20 to 103, but we were -- we discussed the sensitive categories would be between Paragraphs 57 to 73.

And this is -- this is -- this is the data that Oracle says it has that it collects and that it makes available. So this -- this raises a very strong inference that Oracle has actually collected this -- this information on plaintiffs. Plaintiffs know that Oracle has collected information on them. It knows that it's created profiles on them.

Oracle explains to the world that it collects and sells this sensitive information, and this -- this is sufficient to articulate under ***Facebook Tracking***, under ***Carpenter*** that there is a reasonable expectation of privacy that has been violated.

THE COURT: So seguing to the standing issue, what is -- because it's sort of a mass of information that you allude to all sorts of different types of data that may be collected, where are the averments that identify the injury that is being suffered?

Because some of it is -- it's not -- it's a -- because of the scope of the material, one would assume there might be some instances where they -- you would allege or aver injury and others where there wouldn't be any injury. So what is -- what is the injury that the plaintiffs here are alleging?

MR. RUDOLPH: So, first, I want to be clear that plaintiffs are seeking to recover for harms that have already occurred. Oracle focuses quite a bit on the notion of speculative future harm. There is future harm involved, but that is not something that plaintiffs need to rely on for standing.

THE COURT: So where would I look in your Complaint for where there are averments of the injury that has already been incurred?

MR. RUDOLPH: So the -- first, plaintiffs are entitled to statutory damages due to the violations of CIPA and ECPA. Those -- the violations of those statutes --

THE COURT: That's a very interesting question that's been litigated up one side and down the other; whether or not a statutory damage -- if it's subject to statutory damages, that

supplies injury in fact. And it is not self-evident.

And I know there's a lot of law. I have to go back and look. I had a case years ago that went up and I think the Supreme Court at some point dealt with this question. The presence of statutory damages, I concluded in the opinion that I wrote years ago was not -- did not supply the injury in fact element; that it was simply a damage amount.

Now, the case law may have evolved such that that's no longer right and, you know, you may be -- if you're going to tell me, "No, no. Now statutory damages is enough to show injury in fact," I'm -- you may be right. I'd have to go back and look at it, but I -- I thought there was some problems with the statutory damage being the thing you're pointing to for injury.

MR. RUDOLPH: It's not just statutory damages, but the violation of the statute itself is sufficient to confer standing. It's a sufficient concrete interest that -- injury to confer standing. And there's three cases that we cite that discuss this specifically in the context of CIPA and ECPA. It's ***Facebook Tracking***, ***Campbell vs. Facebook***, and ***Eichenberger***, which are all Ninth Circuit cases that discuss a notion that when you have the violation of a statute that embodies these historical rights of privacy, that that in and of itself is sufficient to confer standing. I think that's essentially black letter law in the Ninth Circuit at -- at this

point.

THE COURT: But you don't think you have to aver in your Complaint for Article III standing purposes, you don't have to identify specific injury? You just say: Well, the statute's been violated. These all we need to do?

MR. RUDOLPH: I would say that I don't think we need to allege a specific harm beyond the intrusion itself that the violation of the statute represents.

Again, ***Facebook Tracking***, the court notes that the purpose of these laws or what -- why they were passed was to protect these historical privacy rights; and that once -- once that right has been violated, the tort, if you will, has been complete and there is no --

THE COURT: Okay. Well, I'll go back and look. I have to concede I don't think that's how I thought the law stands at the moment, but I will -- I will go back and look.

And while we're on that subject, just to pick it up, because we are talking about injury in a standing perspective, 17200 is -- has more narrow and demanding standing demonstration; and I don't think there's any doubt when, you know, ***Kwikset*** is the great case, that you've got to show economic injury. So where is that in the 17200 claim?

MR. RUDOLPH: We do allege, Your Honor, that plaintiffs' data has value and that they've lost that value about when their data was wrongfully taken. This is separate

from the unjust enrichment claim.

THE COURT: But doesn't that get you into the thicket of -- that Ms. Cheung is complaining about, that it's just an amorphous set of averments about, well, if you're going to say there's economic value in particular information, don't you have to be more specific about the information? You're sort of suggesting: Well, in this great mass of material information that's being retrieved, there must be economic value in there somewhere. Is that enough for a 17200 claim?

MR. RUDOLPH: Under the -- under the *Brown* and *Calhoun* cases, that -- that is enough; that we've alleged the various types of data that we think on information and belief has been extracted from our plaintiffs, and we allege that that data has value that they've lost.

I think under *Brown* and *Calhoun* and also the *Klein vs. Facebook* case, that that is sufficient to confer standing under 17200.

THE COURT: Okay. Will you -- will you go for me to the wiretap and the CIPA claim and -- claims and with particular attention to the question of the -- on the Wiretap Act, the argument that we heard a little while ago that, you know, one-party consent dooms your claim?

MR. RUDOLPH: Yes.

So as we -- we cite several cases, including the *Revitch* case and also the *Graham vs. Noom* case, which -- which

plaintiff -- Oracle themselves cited, that where you have a situation where you have an independent party that is taking data and doing independent processes and engaging in independent activity using that data, that it's not a third party.

In ***Graham vs. Noom***, the Court distinguished the two other that were sort of engaged in the interception and explained why they weren't, quote/unquote, "service providers." One was NaviStone, which is known as a data broker, and there's cases that describe it that way, and that it was compiling profiles on people and selling that information.

And then the other was ***Facebook*** and the ***Facebook Tracking*** case, which, likewise, was taking information from websites and that it collected on websites with a -- with a plug-in that was on the website and then creating profiles and selling that information. And so in those -- in those cases, the courts said: This is not a mere service provider. This is a third party that is taking the data and also using it for some -- some other purpose.

So I -- I don't think -- I don't think -- I think it's fairly straightforward that the party exception does not apply and also the court in ***Facebook Tracking*** goes into a similar analysis of this question of when you have a plug-in that extracts data and copies it and sends it off to a third party, you're not -- you're not a -- that's not a party, that's not

somebody who's simply providing that information, providing some transitory service for the website operator to utilize. So the party -- the party exception I think does not apply there.

With respect to the one-party consent statute -- first of all, we do not concede that the websites consent to this -- to this conduct. I think for the reasons that Judge Koh articulated in the -- I believe the ***Brown*** case, there's -- there just isn't enough information out there and couldn't be enough information for these websites to really understand what Oracle is doing when it intercepts their data.

Now, our claims don't rely on that interpretation, but I just wanted to be clear that we're not conceding that; but this is where the exception to the exception applies, because Oracle is engaged in independent tortious conduct that is not simply -- we're not alleging that simply the act of the interception, which is a wiretap violation, is tortious, which it is, but it also engages in this tortious conduct of creating these profiles involving sensitive information and selling it to third parties.

And the ***Sussmann*** case says that the fact that Oracle might have a, quote/unquote, "legitimate reason" to collect that information doesn't sanitize the tortious purpose. So the fact that it's seeking profit doesn't sanitize the tortious aspect of its activity.

And, in fact, in ***Sussmann*** the court gave an example of the type of activity that gives rise to the crime tort exception and that's blackmail. Blackmail is sort of by definition to make money. So it can't simply be that if the goal is to make money, then the crime tort exception doesn't apply full stop.

In addition, in ***Brown vs. Google***, Judge Koh found under very similar factual circumstances that the crime tort exception did apply, and the Court said (as read):

"The association of plaintiffs' data with pre-existing use of profiles" -- which is exactly what we allege -- "is a further use of plaintiffs' data that satisfies this exception."

And then the Court said (as read):

"Plaintiffs have adequately alleged that Google's association of their data with pre-existing user profiles violated state laws, including things like intrusion upon seclusion and invasion of privacy."

So there's -- I think there's very rock-solid authority that the crime tort exception does apply here.

THE COURT: Why don't you shift focus for a moment to the, for want of a better way to encapsulate it, the arguments that Ms. Cheung was making about extra-territoriality and I pushed back just saying it's perhaps not something to be ferreted out on a Motion to Dismiss, but -- and I think she's probably right, there are certainly case law where those issues

have been addressed at the pleading stage.

So what's your position with respect to why all these non-California players out there are in the right place?

MR. RUDOLPH: First, I -- we agree that this is not the appropriate time for -- the appropriate stage of the case to make that determination; but under the framework in *Mazza* and *Stromberg*, the -- once -- the plaintiffs have the burden to show that there's a sufficient aggregation of contacts with the state, and we've done that. We've alleged in some detail that the -- that the headquarters for much of the time period during which this happened was California. We've alleged that the conduct conceived and -- was conceived and emanated from California.

Oracle, what I heard Ms. Cheung say was that there is perhaps a factual dispute about whether or not that's actually the case, and that goes -- just demonstrates that -- that what would be necessary then would be discovery, but Oracle did not -- did not contest jurisdiction or venue in this case.

So those allegations have been made and when we've done that sufficiently, then the burden shifts on Oracle to show under the three-prong governmental interest test that the laws of the other states should displace California's interest.

And I think we're really clear that Oracle just didn't -- hasn't met that burden. It looks at the laws of two states. It suggests some superficial differences. It doesn't engage in

a rigorous analysis at all, and it just hasn't met its burden. It hasn't provided the Court with the tools to actually engage in a choice of law analysis.

A choice of law analysis can be a very detailed inquiry that involves sometimes expert testimony regarding the differences between laws, it would be differences of the states. That is something that is more appropriately done on a more developed record.

So I think as an initial matter, it's just -- Oracle has not met its burden to overcome the presumption that California law should apply here.

THE COURT: Okay. Anything -- before I go back to Ms. Cheung, anything else?

MR. RUDOLPH: There is. I would like to address this consent issue, Your Honor.

THE COURT: Yes.

MR. RUDOLPH: Consent -- consent is not an actual defense to any of Oracle's -- to any of these -- of these -- I'm sorry.

Consent is not something that's at issue in this motion to consent, whether or not the plaintiffs have actually consented. The plaintiffs have not consented. They allege that in the Complaint. Oracle does not make any effort to contest that. And so that's just -- as a matter of the pleadings, that's the states.

But the bigger issue is that really based on the way Oracle operates and the expansiveness of the -- of the level of surveillance, that there really isn't a way that anybody -- a reasonable person could actually consent to this. It's just -- it's too complicated. There's too many unknowns. There's too many -- too many variables that a reasonable person just wouldn't be able to do it.

And I'll just point to Your Honor's sort of memorable statement in the ***Rodriguez*** case that the average internet user is not a full-stack engineer and he shouldn't be treated as one when a company explains where the digital data goes.

And I think the level of detail that somebody would need to be really informed and understand what Oracle was doing with their data, which we, you know, lay out in 70 pages in our Complaint, would require them to essentially have that -- that level of expertise.

And there actually is one other point I'd like to address, which is this question of whether or not the conduct is highly -- highly egregious.

I think that we allege and demonstrate through the -- and obviously this is related not just to legislators and commentators, et cetera, but also just based on the concerns that are embodied in the California Constitution, that what Oracle is engaging in has reached a level where it is highly egregious, and that -- that this is generally recognized as a

major societal problem.

And one of the -- one of the reasons for that is because it really -- this level of surveillance that when it's so pervasive and unknown in the way that Oracle does -- does it, really impinges on people's autonomy and their ability to function in a democracy.

And this ties in with the consent issue because people can't consent to this level of pervasive surveillance and manipulation, which is what the surveillance is for, because it affects other people based on the way a democracy works. People who have a right to vote can't sort of be unwillingly consenting to give up their autonomy.

And -- so, I mean, this is -- these are all reasons that this is highly egregious.

Now, I would say the final point is that this question of whether or not it's highly egregious is a factual determination for the fact finder. And I know Your Honor has found that in other cases, that ***Facebook Tracking*** case noted that, that that's really the stage at which a finder of fact or a jury needs to come in and decide whether or not this conduct is highly egregious according to social norms.

And that's what we're seeking in this case, to have -- have a jury decide whether or not what Oracle is doing is a violation of these fundamental privacy rights that have been around for 50 years at least and should be enforced now against

this sort of surveillance.

THE COURT: Thank you.

Ms. Cheung, you get, being the moving party, the last words.

MS. CHEUNG: Thank you, Your Honor.

I'll start with the ballot measure that plaintiffs rely so heavily on for the -- to support the general right to privacy.

I note that that ballot measure was passed in 1972, which predated all of the cases that we cite, which say app device history -- you know, contact information, app device history, browsing history, none of that rises to the level of an invasion of privacy.

So we all know, even -- even post this ballot measure, that there is certain types of information for which the society accepts that we do not have a -- it is not an egregious breach of privacy in order to share that information. Address information is, of course, an example that Your Honor gave, and to the extent that address is combined with the fact that someone owns an iPhone doesn't now make that aggregate data an egregious invasion of privacy. So that's one.

The other point to make is on ***Facebook Tracking***, because plaintiffs rely on it so heavily. But in addition to the fact that ***Facebook Tracking*** was extremely different in that Facebook did make an affirmative representation that it would not collect the information that it allegedly did collect, it also

involved the type of sensitive information that courts have said are a factor in determining whether there's an invasion of privacy.

Facebook had access to users' profiles, which allegedly included potentially religious and political information of the type of sensitivity that is -- that is considered in invasion of privacy claims.

There is nothing other than conclusory allegations in this case that Oracle ever collected anything that is -- that rises to that level of sensitivity.

And it's notable that plaintiffs have alleged that Oracle allegedly gave them information that shows that it collected certain information on -- on the plaintiffs, but the plaintiffs don't then go on to say: And that information shows that this type of sensitive information was collected. They claim they have it, they claim that Oracle gave it to them, and they don't actually say that it included any sensitive information. So they rely only on conclusory generic allegations to meet that sensitivity threshold.

Finally, Your Honor -- well, actually, let me touch on the ECPA claim briefly because the crime tort exception just simply doesn't apply. They've really made no allegations that there was any kind of criminal or tortious activity independent of the alleged interception, which is what they would need to plead and prove in order to show a federal wiretap claim.

Plaintiffs raised the example that blackmail might have risen to the level of the crime tort exception, but they certainly don't allege that here or any other kind of crime or tortious behavior that's independent that would serve to be the exception to the exception, which is that ECPA is a one-party consent statute and the one party, the website operator's consent is sufficient for a defense.

With respect to consent, they -- plaintiffs have argued we don't contest that plaintiffs didn't consent, but of course we do. Our point is that they don't actually tell us which website they allegedly put information into that then was shared with Oracle so that we can determine whether, in fact, they did consent or not. Because when they input information allegedly into websites, those websites were required to get the required consent; and as far as Oracle's concerned, that is what the website operators did.

They do not allege otherwise. They don't allege they got into this website, they entered this type of information that was sensitive, and they did not consent when there was a cookie pop up or there was a request to give that consent. Plaintiffs never alleged that they did not give consent to these websites in order to share data.

THE COURT: Isn't it their contention that whether or not there was some consent vis-a-vis these third-party players, that that doesn't redound to the benefit of Oracle?

So the question really is -- I don't think -- granted, it doesn't seem to me that they're contesting that perhaps some of these third parties did get some form of consent perhaps, but if they did or they didn't, it's not to Oracle's benefit.

MS. CHEUNG: The only way to answer that question, Your Honor, is to look at the specific consent language of that website operator. Because there are websites that will draft their consent language in ways to encompass service providers that they have used in order to track analytics. And if the consent language is broad enough to cover service providers like Oracle, that consent does redound to Oracle.

So the question is: Which website did they go on and they gave this -- to give this information and what was the scope of that particular website's consent? We don't know because they don't allege it. They just generically say: We went onto websites. Everyone has to go on the internet. And then information somehow gets to Oracle, but there's no traceability and several missing gaps to meet that causation link.

And then --

THE COURT: But at the pleading stage would a plaintiff need to -- in pleading this kind of conduct have completed -- effectively what I hear you saying is they would have to complete all their discovery before they bring a Complaint almost.

I mean, no plaintiff is going to know every website that

Oracle may have been interacting with through which your -- these plaintiffs were providing data. They're not going to know that at this stage of the case.

So I understand your argument that it's -- and it's all -- it's not on a spectrum. They just haven't gotten, from your perspective, even within the bounds of discussion, but they're never going to be able to provide the information at the outset of the case that you're saying they would have to provide.

MS. CHEUNG: Yeah, and understood, Your Honor. We're not -- we're not certainly suggesting that there needs to be the entire exhaustive list of every single website they ever went onto. That is not what we're suggesting. But they don't even name one. They don't even name one for which they don't consent, and they allege that they have this information allegedly from Oracle that was collected but don't make any connection between where that -- how Oracle got that information and/or whether it's in any way sensitive and how that connection got -- came from the consumer where, you know, it ultimately got to Oracle.

So they have some information and they have noticeably omitted where that causation link lies. So not even a single -- not even a single website. That does not suffice.

And then my final point, Your Honor, is on extra-territoriality because plaintiffs are arguing that it's not something that can be decided at this stage. But even

based on the allegations of the Complaint, especially when they are relying so heavily on Oracle's headquarters, which during the time period that they allege information was shared, Oracle's headquarters were not, in fact, even according to their Complaint, not, in fact, in California, these -- these allegations in the Complaint are sufficient in order to make a determination on whether California law can apply to a global class.

THE COURT: Going back to the initial discussion about standing, Article III standing, we had -- I had a discussion with Mr. Rudolph about statutory damages and the impact of statutory damages, whether or not that could perhaps be a basis on which you don't need to be more specific in terms of injury, do you want to comment on that?

MS. CHEUNG: Yes. Thank you, Your Honor.

Although there is I think authority that could go either way on this, the point I will make there and the point that I think is important is that *TransUnion* is the recent Supreme Court case that addresses this issue most recently; and under *TransUnion*, a mere violation of a statute does not suffice for jury under Article III.

I think I'm familiar with the cases Mr. Rudolph is referring to, but they predate *TransUnion* and *TransUnion* is now the Supreme Court authority on this issue.

THE COURT: Okay. Well, I will go back with the

benefit of your helpful argument and I will go through it and get you an order.

MS. CHEUNG: Thank you, Your Honor.

MR. RUDOLPH: Thank you, Your Honor.

THE COURT: Thank you very much.

(Proceedings adjourned at 2:42 p.m.)

CERTIFICATE OF REPORTER

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

Debra L. Pas, CSR 11916, CRR, RMR, RPR

Friday, March 10, 2023

20